FRAUD TRENDS

GLOBALLY AND IN SOUTH AFRICA

JANUARY 2021

Newsletter #2

marketing@rmgforensics.com

www.rmgforensics.com

RMG FORENSIC SERVICES (Pty) Ltd.

CELEBRATING 10 YEARS OF EXCELLENT SERVICE

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

RMG Forensic Services is proud to employ Certified Fraud Examiners

Index

Subject for this fraud newsletter version 2/2021:

CYBER SECURITY IN YOUR ORGINIZATION

Foreword _____ 2

What is cyber security? _____ 3

What recent data breaches reveal about cyber security in South Africa _____ 3

Best defense_____ _____ 4

What is a cybersecurity threat? _____ 4

Where do these threats come from? _____ 5

Common Cyber Security Threats_____ 6

10 Cybersecurity Tips and Best Practices_____ 7

Statistics_____ 8

Foreword

As part of the Fraud Awareness initiative of the MRG Group to its members this monthly Fraud newsletter would assist with the most current Fraud Trends detected in the industry as well as practical advice to proactively remedy this.

In this month's fraud newsletter version 2/ 2021 we cover the subject at hand: cyber security threats. We will explain the definition and these modes operandi of the fraud and provide tips on how to prevent it.

In the next edition newsletter version 3 / 2021 in the first quarter of the year we will define cyber security threats in the South African and in the global context.

What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories:

- Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect.
- Information security protects the integrity and privacy of data, both in storage and in transit.
- Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug-in unidentified USB drives, and various other important lessons is vital for the security of any organization.

What recent data breaches reveal about cyber security in South Africa

2020 has seen well-known local healthcare and financial organisations falling victim to attacks and data breaches or being forced offline.

Local data breaches coincided with high profile attacks and outages experienced by global brands such as Twitter and Garmin, and credit bureau Experian reporting a massive breach that exposed the personal information of up to 24 million South Africans and nearly 800 000 businesses.

“These incidents have brought to light a battle that has been waging quietly in the background,” says RMG Forensic cyber experts. “Cyber criminals –using increasingly sophisticated techniques – are targeting South African public and private sector organisations in orchestrated attacks that could lead to devastating losses in business productivity, reputational damage and revenue.”

Mimecast’s State of Email Security 2020 report revealed that 53% of local organisations reported increased phishing attacks and 46% reported increased incidences of impersonation fraud compared to the previous year, no doubt exacerbated by the COVID-19 pandemic.

“Big or small, any organisation can fall victim to a data breach. As the Experian breach has showed, it is not always computer whizzes that ‘hack’ company data. A clever fraudster posing as a trusted partner or supplier can just as easily get away with valuable internal data that can be used in cyberattacks.”

In addition, our cyber experts say breaches are more common than most realise. “With POPIA now in effect, organisations are duty-bound to disclose breaches. We can expect to see many more reports of data breaches over the coming months.”

Best Defense

To protect themselves from attacks, RMG Forensic advises companies to develop a layered security strategy. "The threat landscape has shifted to the point where organisations need to approach security with three zones in mind. Firstly, at the e-mail perimeter, where security controls can detect and block malicious emails. Next, inside the organisation, which includes protecting against internal threats and awareness training. Finally, beyond the perimeter, where cyber criminals are finding great success with brand impersonation that can trick unsuspecting customers and partners into offering up important information or into making payments to fraudulent bank accounts."

Studies suggest human error plays a role in 90% of all data breaches

Furthermore, RMG Forensic advises to focus on empowering people, because no matter how good a company's defenses are, humans are the weakest link, and without a 'strong human firewall', they remain susceptible to data breaches.

Studies suggest human error plays a role in 90% of all data breaches. Mimecast found that users who had been exposed to cyber awareness training were over five times less likely to be taken in by certain types of fraud.

In conclusion, RMG Forensics' cyber experts say one of the most effective security strategies is conducting regular and on-going awareness training to ensure staff can identify and avoid risky online behavior. "Organisations also need to identify high-risk employees or job titles, such as those in finance, that attackers are likely to target, and ensure they invest in additional awareness training and security controls for such employees."

What is a cybersecurity threat?

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors.

Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

Where do these threats come from?

- **Hostile nation-states:**
  National cyber warfare programs provide emerging cyber threats ranging from propaganda, website defacement, espionage, disruption of key infrastructure to loss of life. Government-sponsored programs are increasingly sophisticated and pose advanced threats when compared to other threat actors. Their developing capabilities could cause widespread, long-term damages to the national security of many countries including the United States. Hostile nation-states pose the highest risk due to their ability to effectively employ technology and tools against the most difficult targets like classified networks and critical infrastructure like electricity grids and gas control valves.

- **Natural disasters:**
  Natural disasters represent a cyber threat because they can disrupt your key infrastructure just like a cyber-attack could.

- **Accidental actions of authorized users:**
  Some of the biggest data breaches have been caused by poor configuration rather than hackers or disgruntled insiders.

- **Hacktivists:**
  Hacktivists activities range across political ideals and issues. Most hacktivist groups are concerned with spreading propaganda rather than damaging infrastructure or disrupting services. Their goal is to support their political agenda rather than cause maximum damage to an organization.

- **Terrorist groups:**
  Terrorist groups are increasingly using cyber-attacks to damage national interests. They are less developed in cyber-attacks and have a lower propensity to pursue cyber means than nation-states. It is likely that terrorist groups will present substantial cyber threats as more technically competent generations join their ranks.

- **Corporate spies and organized crime organizations:**
  Corporate spies and organized crime organizations pose a risk due to their ability to conduct industrial espionage to steal trade secrets or large-scale monetary theft. Generally, these parties are interested in profit-based activities, either making a profit or disrupting a business's ability to make a profit by attacking key infrastructure of competitors, stealing trade secrets, or gaining access and blackmail material.

- **Disgruntled insiders:**
  Disgruntled insiders are a common source of cyber-crime. Insiders often do not need a high degree of computer knowledge to expose sensitive data because they may be authorized to access the data. Insider threats also include third-party vendors and employees who may accidentally introduce malware into systems.

- **Hackers:**
  Malicious intruders could take advantage of a zero-day exploit to gain unauthorized access to data. Hackers may break into information systems for a challenge or bragging rights. In the past, this required a high level of skill. Today, automated attack scripts and protocols can be downloaded from the Internet, making sophisticated attacks simple.

Common Cyber Security Threats

- **Malware:** Malware is software that does malicious tasks on a device or network such as corrupting data or taking control of a system.
- **Spyware:** Spyware is a form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.
- **Phishing attacks:** Phishing is when a cybercriminal attempts to lure individuals into providing sensitive data such as personally identifiable information (PII), banking and credit card details and passwords.
- **Distributed denial of service (DDoS) attacks:** Distributed denial of service attacks aim to disrupt a computer network by flooding the network with superfluous requests to overload the system and prevent legitimate requests being fulfilled.
- **Ransomware:** Ransomware is a type of malware that denies access to a computer system or data until a ransom is paid.
- **Zero-day exploits:** A zero-day exploit is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching the flaw.
- **Advanced persistent threats:** An advanced persistent threat is when an unauthorized user gains access to a system or network and remains there without being detected for an extended period.
- **Trojans:** A trojan creates a backdoor in your system, allowing the attacker to gain control of your computer or access confidential information.
- **Wiper attacks:** A wiper attack is a form of malware whose intention is to wipe the hard drive of the computer it infects.
- **Intellectual property theft:** Intellectual property theft is stealing or using someone else's intellectual property without permission.
- **Theft of money:** Cyber-attacks may gain access to credit card numbers or bank accounts to steal money.
- **Data manipulation:** Data manipulation is a form of cyber-attack that does not steal data but aims to change the data to make it harder for an organization to operate.
- **Data destruction:** Data destruction is when a cyber attacker attempts to delete data.
- **Man-in-the-middle attack (MITM attack):** A MITM attack is when an attack relays and possibly alters the communication between two parties who believe they are communicating with each other.
- **Drive-by downloads:** A drive-by download attack is a download that happens without a person's knowledge often installing a computer virus, spyware or malware.
- **Malvertising:** Malvertising is the use of online advertising to spread malware.
- **Rogue software:** Rogue software is malware that is disguised as real software.
- **Unpatched software:** Unpatched software is software that has a known security weakness that has been fixed in a later release but not yet updated.
- **Data center disrupted by natural disaster:** The data center your software is housed on could be disrupted by a natural disaster like flooding.

10 Cybersecurity Tips and Best Practices

1. **Keep software up to date:**
   Software companies typical provide software update for 3 reasons: to add new features, fix known bugs, and upgrade security. Always update to the latest version of your software to protect yourself from new or existing security vulnerabilities.

2. **Avoid opening suspicious emails:**
   If an email looks suspicious, do not open it because it might be a phishing scam. Someone might be impersonating another individual or company to gain access to your personal information. Sometimes the emails may also include attachments or links that can infect your devices. Links can easily be disguised as something they are not, so it is best to double check before you click on a hyperlink. On most browsers, you can see the target by hovering over the link. Do this to check links before you click them. The key to making cybersecurity work is to make sure your employees are well tried, in sync, and consistently exercising security best practices. One mistake from an improperly trained employee can cause an entire security system to crumble.

3. **Use a secure file sharing solution:**
   The files you share are only as secure as the tools you use to share them with. Adopt a secure file sharing solution to encrypt your files while they are in transit and at rest to prevent unauthorized access and keep your files safe.

4. **Use anti-virus and anti-malware:**
   If you are connected to the web, it is impossible to have complete and total protection from malware. However, you can significantly reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware installed on your computers.

5. **Do not be lazy with your password:**
   Put more effort into creating your passwords. You can use tool like howsecureismypassword.net to find out how secure your passwords are.

6. **Scan external storage devices for viruses:**
   External storage devices are just as prone to malware as internal storage devices. If you connect an infected external storage device to your computer, the malware can spread. Always scan external devices for malware before accessing them.

7. **Enable 2-factor authentication:**
   Many platforms now allow you to enable 2-factor authentication to keep your accounts more secure. It is another layer of protection that helps verify that it is you who is accessing your account and not someone who is unauthorised. Enable this security feature when you can.

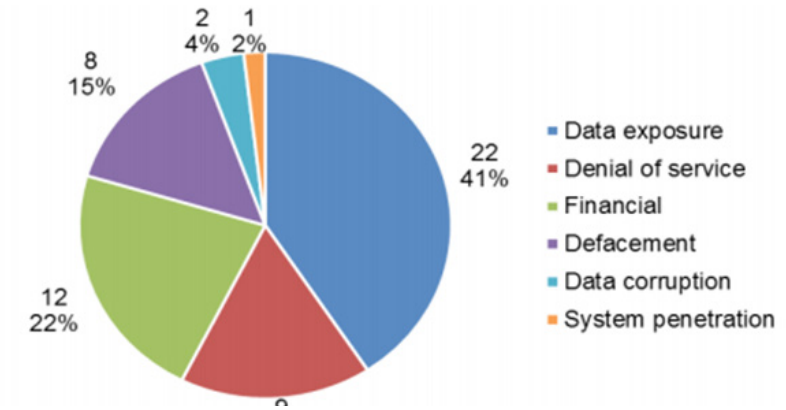
8. **Only store sensitive information in secure places:**
   When storing information online, you want to keep it in a location that cannot be accessed by unauthorised user.

9. **Double check for HTTPS on websites:**
   When you are on a website that is not using HTTPS, there is no guarantee that the transfer of information between you and the site's server is secure. Double-check that a site is using HTTPS before you give away personal or private information.

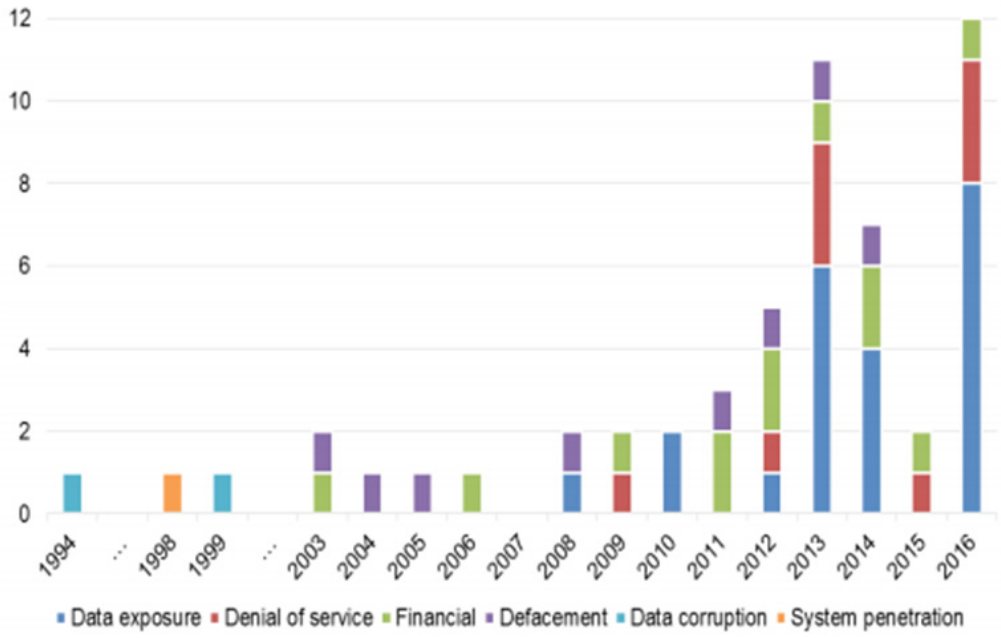
10. **Disable Bluetooth when you do not need it:**
    Devices can be hacked via Bluetooth and subsequently your private information can be stolen. If there is no reason to have your Bluetooth on, turn it off.

Statistics

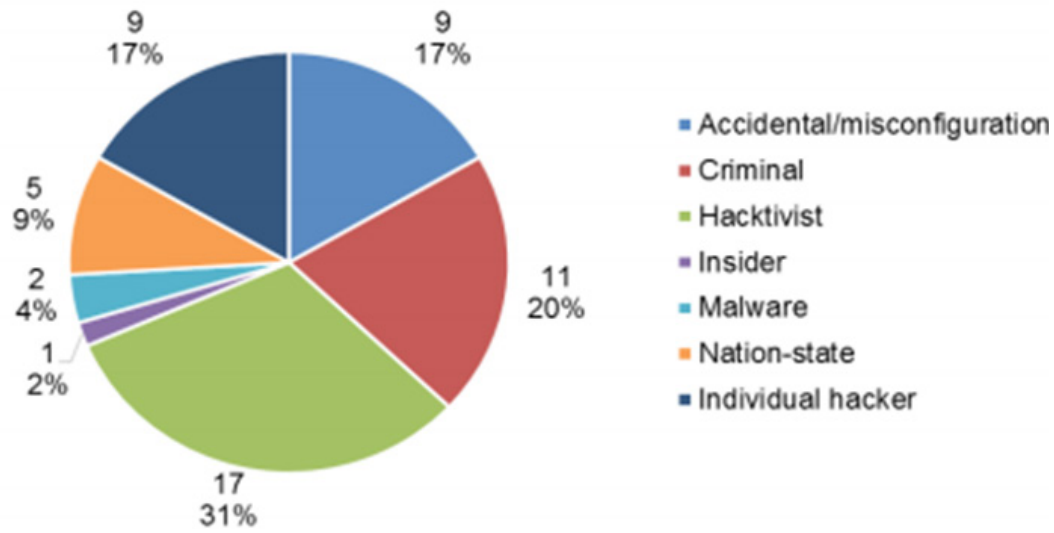
Cyber-incidents related to South Africa were identified through scrutiny of published reports, news items, postings to email mailing lists, cross-referencing via document reference lists, and targeted online searches for additional information on documented incidents. A total of 54 incidents spanning 23 years, from April 1994 to end-2016, were identified. The following figure shows the percentage distribution of the 54 incidents across six impact types. As is evident, data exposure is the most prominent impact type. Financial, denial of service. and defacement are also noticeable.

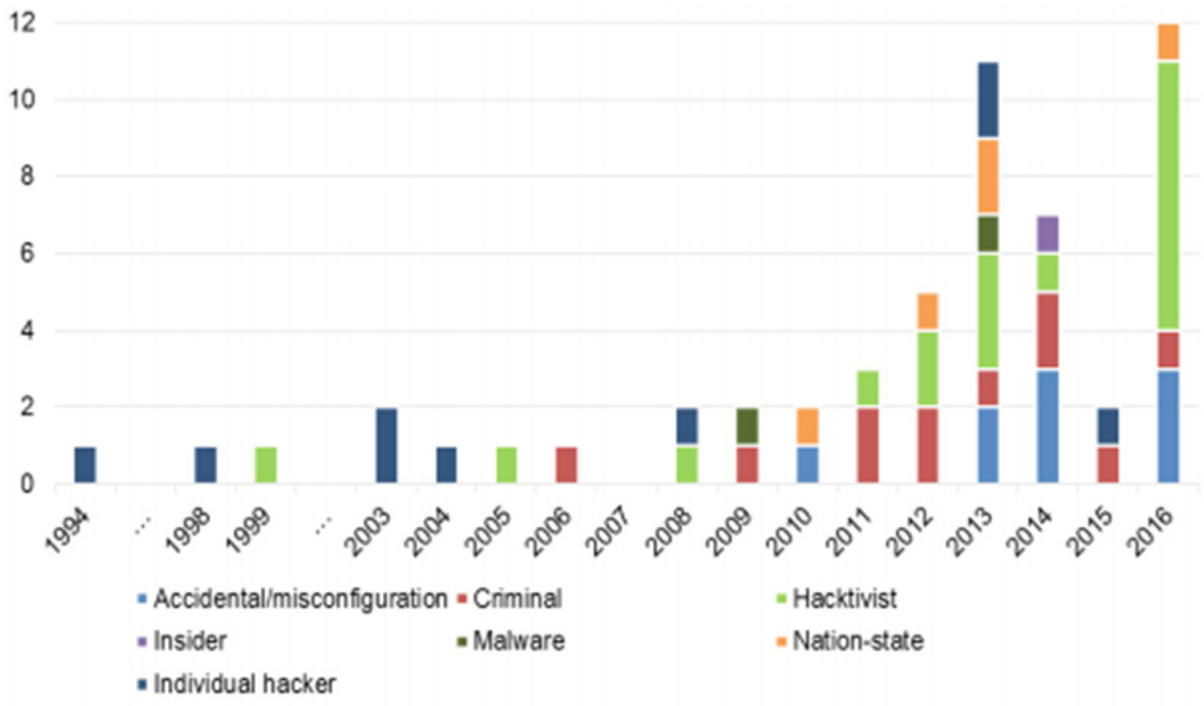


Trends in impact type

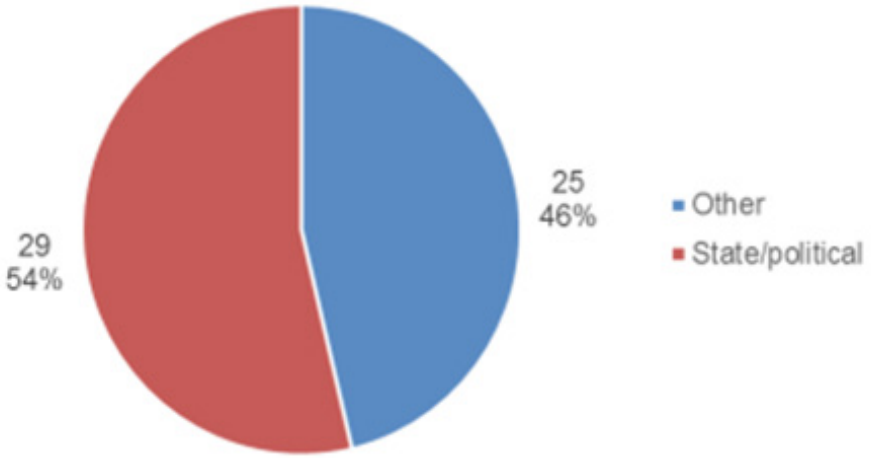


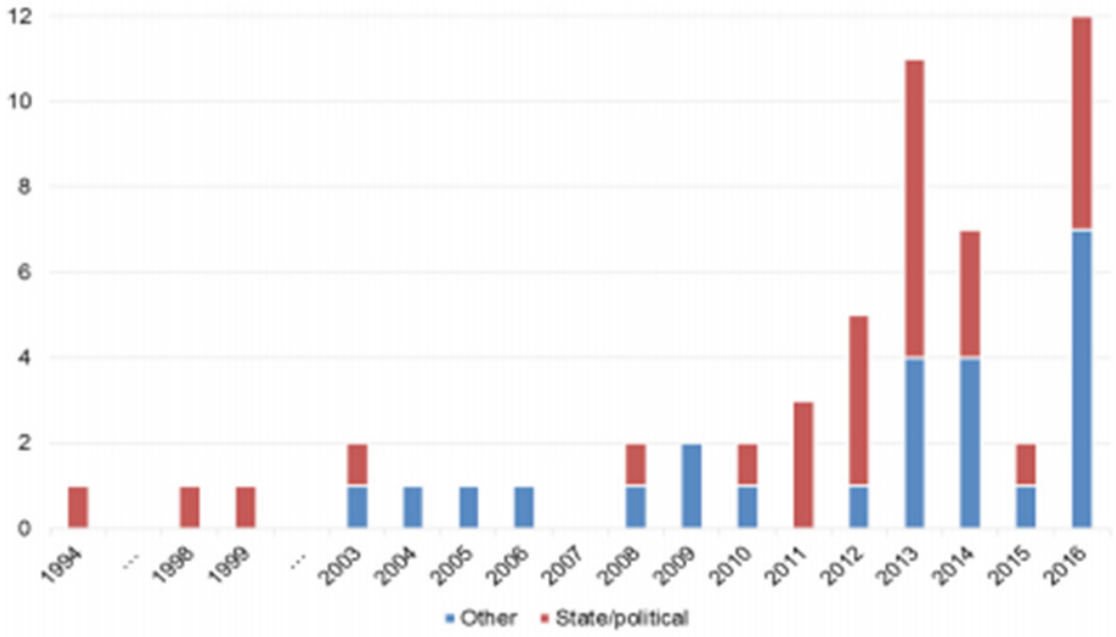
Perpetrator Type





Victim Type


25
46%
29
54%
Other
State/political


12
10
8
6
4
2
0
1994
1998
1999
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
Other
State/political